SAP HCP – Webinar Series 4 SAP User Groups

Moderator: Jos Houben

SAP HCP Digital Future Enabled by SAP HANA Cloud Platform	Prakash Darji	Mar 17
SAP HCP and HEC: How they compare and combine	Uddhav Gupta / Maria Yu	Mar 29
Building new Analytical Solutions on HCP	Jana Richter	Apr 4
Building Cloud extensions with HCP	Filip Misovski	Apr 6
Building on-premise extensions on HCP	Bertram Ganz	Apr 12
SAP HCP – Using HCP for Mobile Apps	Holger Gauss/Dirk Olderdissen	Apr 14
SAP HCP – Addressing Security Concerns	**Martin Raepple**	**Apr 19**

SAP HANA Cloud Platform – A Security Overview

HCP Security Webinar

Martin Raepple, Product Owner SAP HANA Cloud Platform Security

Public

Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

Agenda

SAP HANA Cloud Platform

Authentication, identity federation, single sign-on

Authorization management

API protection

Storing confidential data

User store integration

Secure backend connectivity

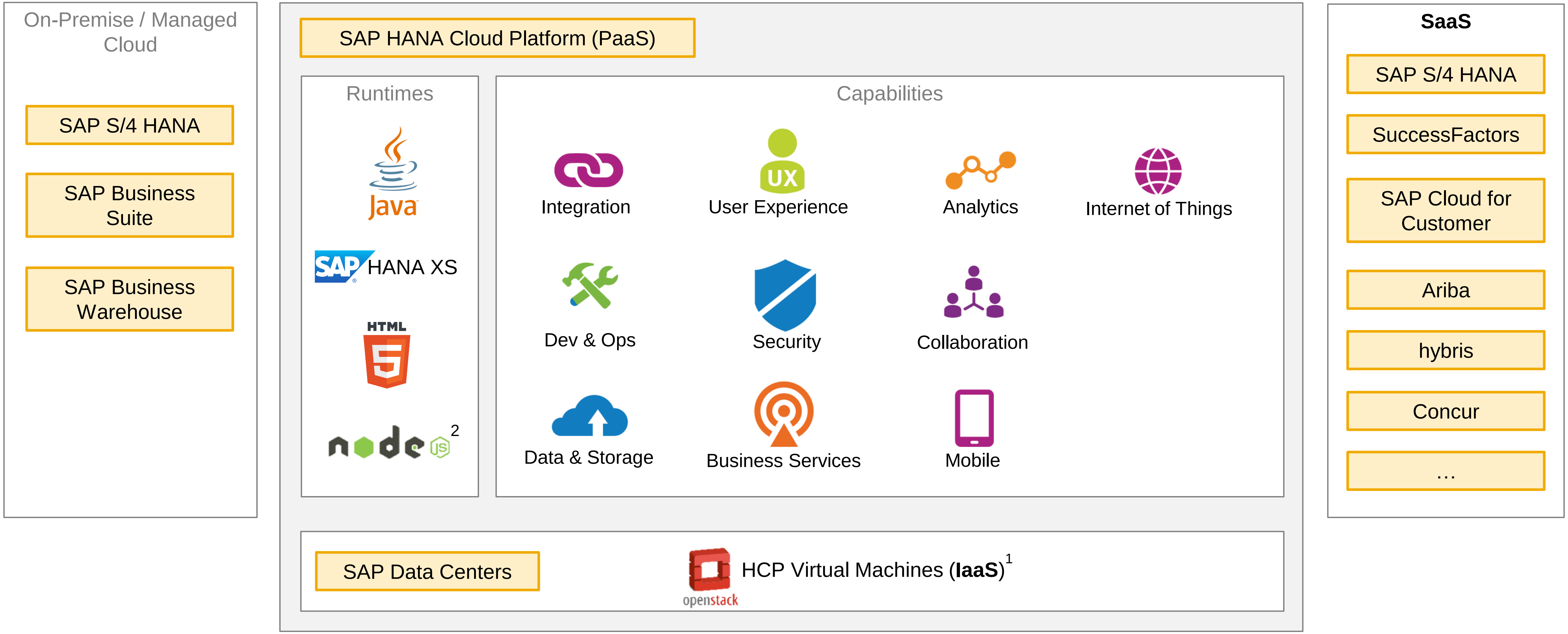
Identity propagation

Summary

SAP HANA Cloud Platform

SAP HANA Cloud Platform

The Platform-as-a-Service (PaaS) for powering cloud applications



On-Premise / Managed Cloud

- SAP S/4 HANA
- SAP Business Suite
- SAP Business Warehouse

SAP HANA Cloud Platform (PaaS)

Runtimes

- Java
- SAP HANA XS
- HTML 5
- node JS[2]

Capabilities

- Integration
- User Experience
- Analytics
- Internet of Things
- Dev & Ops
- Security
- Collaboration
- Data & Storage
- Business Services
- Mobile

SAP Data Centers

openstack HCP Virtual Machines (**IaaS**)[1]

SaaS

- SAP S/4 HANA
- SuccessFactors
- SAP Cloud for Customer
- Ariba
- hybris
- Concur
- …

1) beta functionality 2) planned innovations / future direction

SAP Data Center and HANA Cloud Platform Security Compliance

- Certified operations

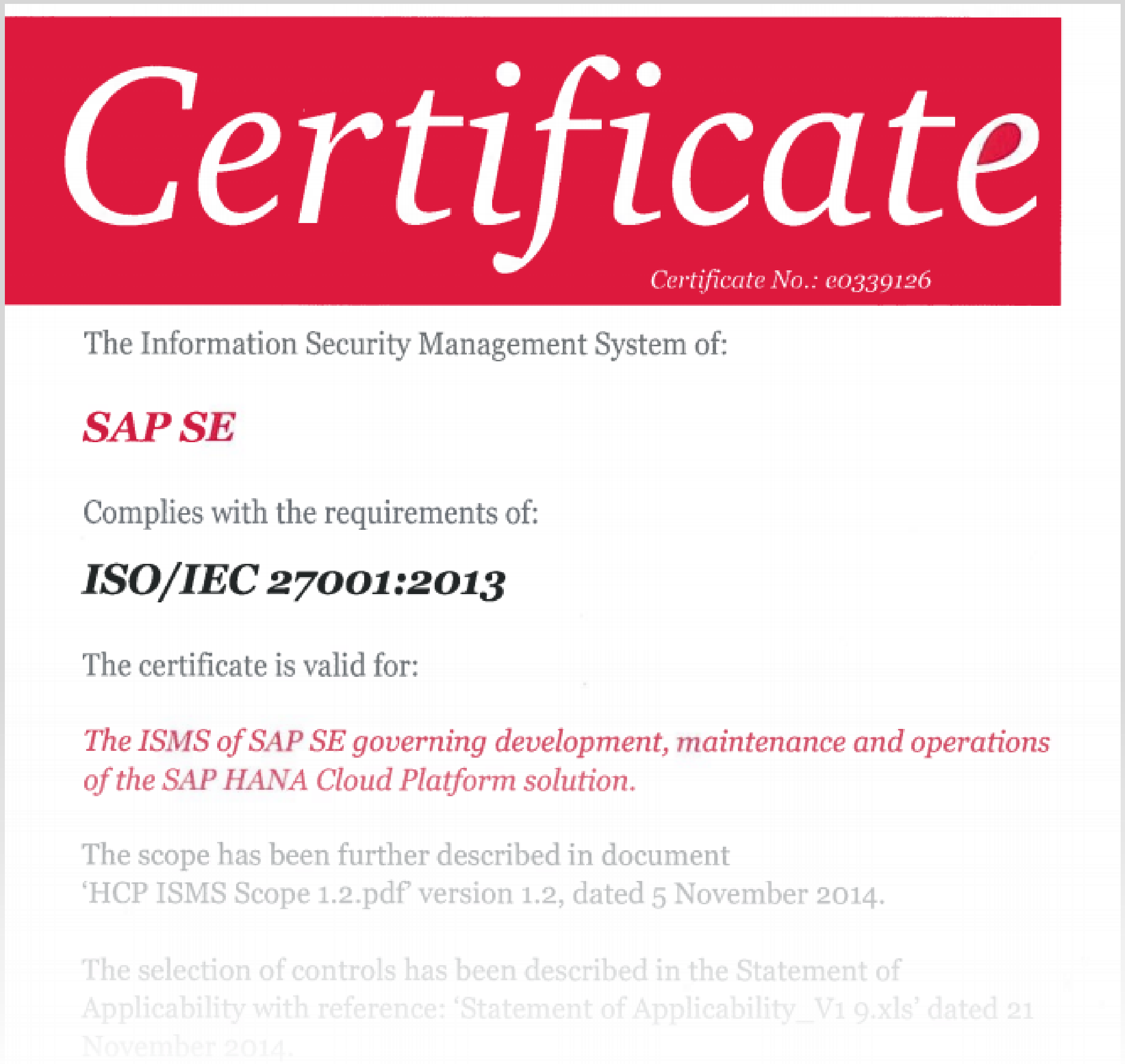
ISO 27001 [1] [3]
Certification for Information Security Management Systems

SOC 1 / SSAE 16 [2] [3]
Statement on Standards for Attestation Engagements No. 16

SOC 2 [3]
Service Organization Controls Report (Attestation report)

ISO 22301 [3]
Certification for Business Continuity Management Systems

- World-class data centers in Americas, EMEA & APJ
- Advanced network security
- High availability and reliable data backup



Certificate

Certificate No.: e0339126

The Information Security Management System of:

SAP SE

Complies with the requirements of:

ISO/IEC 27001:2013

The certificate is valid for:

The ISMS of SAP SE governing development, maintenance and operations of the SAP HANA Cloud Platform solution.

The scope has been further described in document 'HCP ISMS Scope 1.2.pdf' version 1.2, dated 5 November 2014.

The selection of controls has been described in the Statement of Applicability with reference: 'Statement of Applicability_V1 9.xls' dated 21 November 2014.

[1] Certification for SAP HANA Cloud Platform
[2] In progress for SAP HANA Cloud Platform
[3] The same or equivalent certificates are valid at every data center where cloud solutions are run.

SAP HANA Cloud Platform

Major usage scenarios

BUILD

New cloud apps

EXTEND

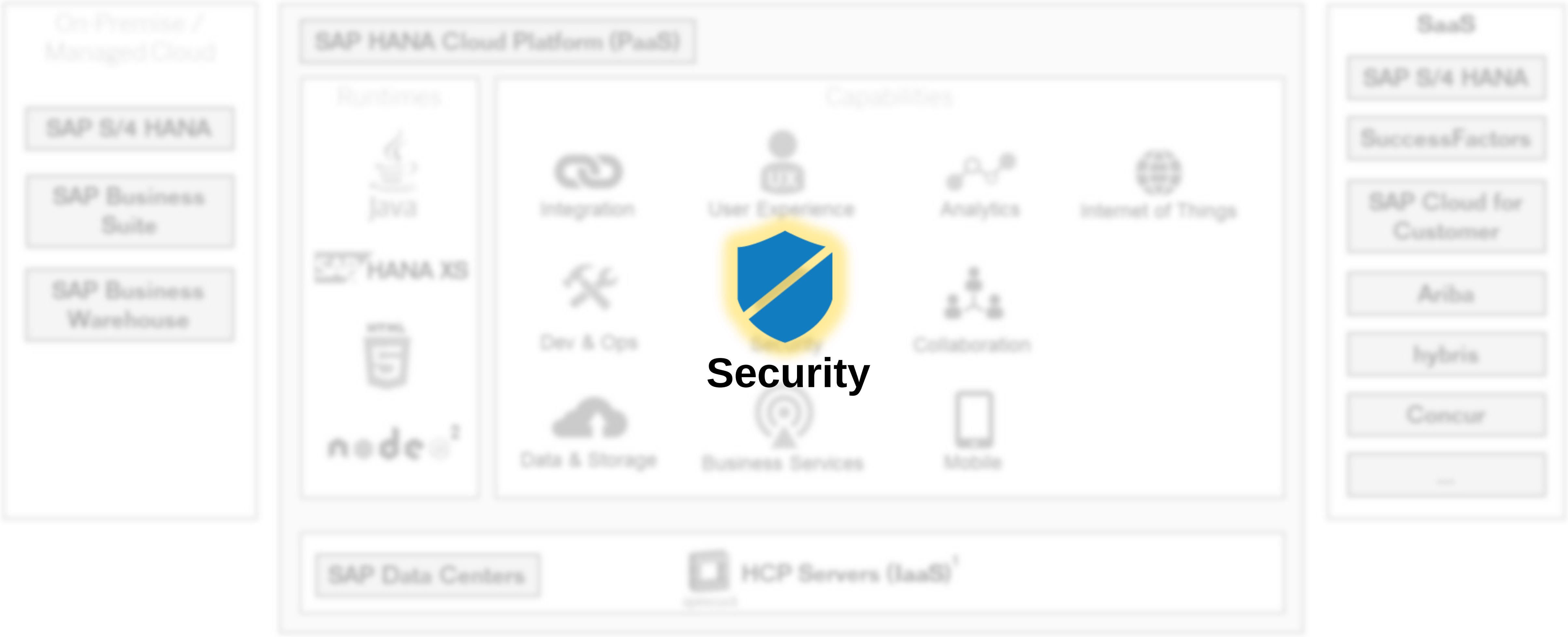
Business apps

INTEGRATE

Everything

SAP HANA Cloud Platform

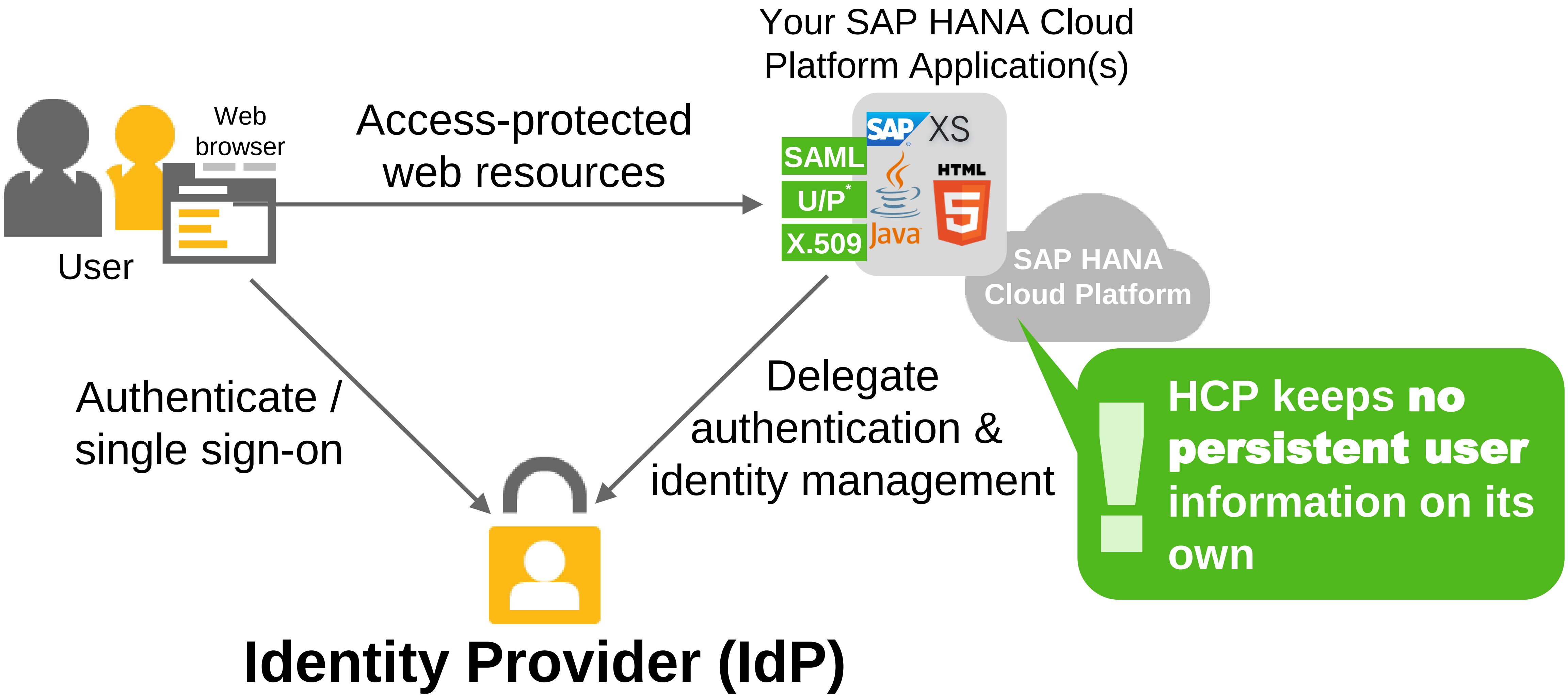
Focus of this session



1) beta functionality 2) planned innovations / future direction

Authentication, identity federation, single sign-on

Federated authentication & SSO in SAP HANA Cloud Platform



Your SAP HANA Cloud Platform Application(s)

Access-protected web resources

Authenticate / single sign-on

Delegate authentication & identity management

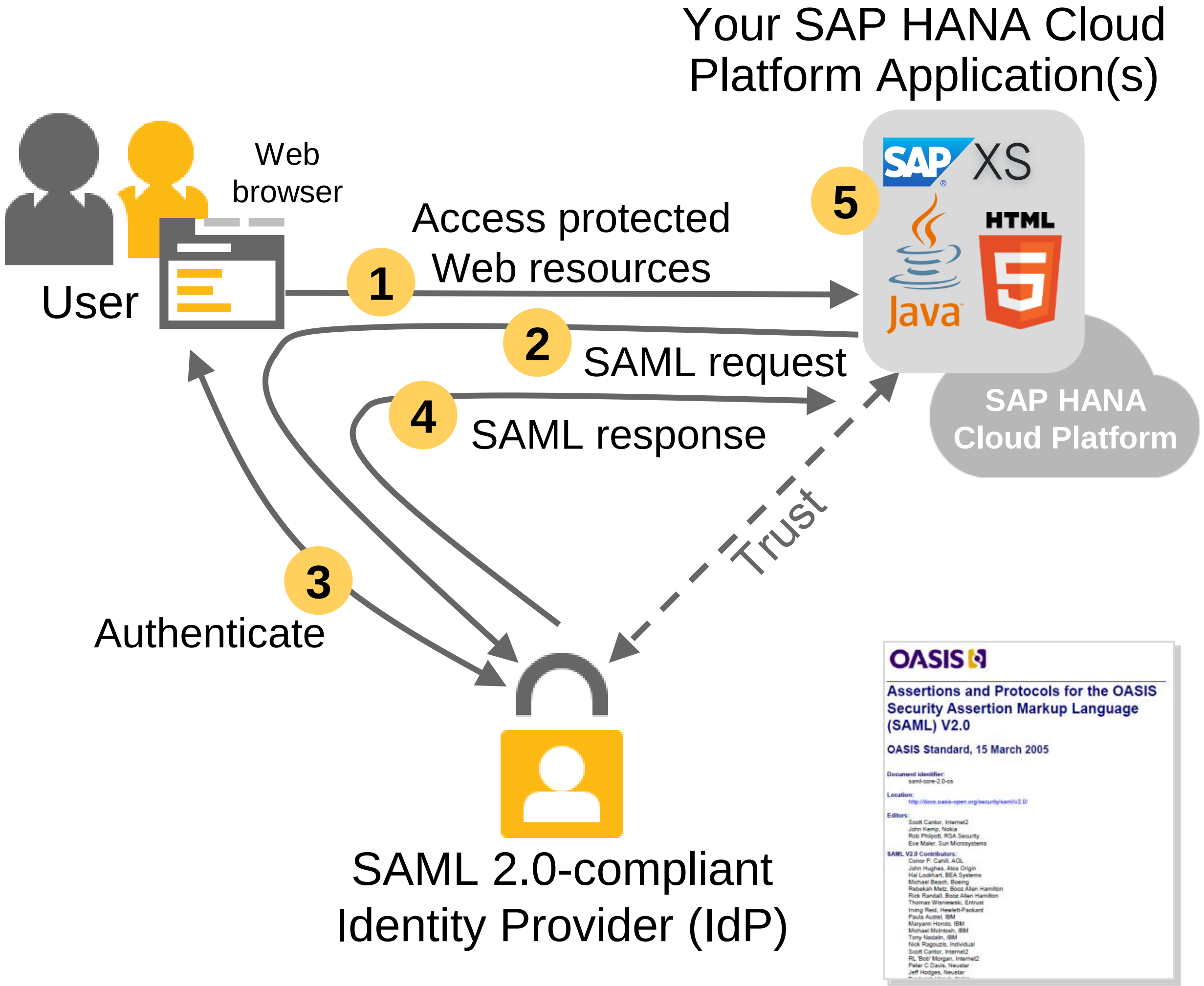
HCP keeps **no persistent user** information on its own

Identity Provider (IdP)

* Username / Password with HTTP Basic Authentication

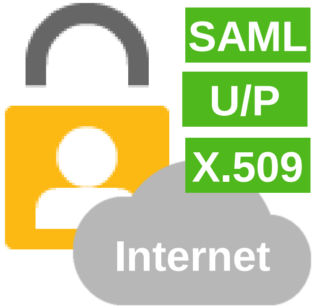
Federated authentication and SSO for browser-based applications with SAML 2.0

1. User accesses protected web resource on SP
2. SAP HANA Cloud Platform Application sends SAML authentication request via **HTTP redirect** to trusted IdP
3. IdP authenticates the user (if not done already)
4. Upon successful authentication, IdP sends an **HTML form** with the SAML response message in a hidden field to the web browser, which (auto)submits it using an embedded **(Java)Script**
5. **User is created** based on information in the SAML response


Your SAP HANA Cloud Platform Application(s)
Web browser
User
SAP XS
HTML
Java
5
1
Access protected Web resources
2
SAML request
4
SAML response
SAP HANA Cloud Platform
Trust
3
Authenticate
SAML 2.0-compliant Identity Provider (IdP)
OASIS
Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
OASIS Standard, 15 March 2005

http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

Identity provider options on SAP HANA Cloud Platform

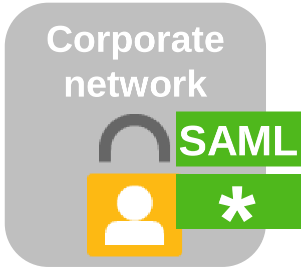


SAP ID Service

- SAP‘s public IdP on the Internet
- Free service, similar to social IdPs
- Shared user base with SCN, SAP Service Marketplace and other public SAP web sites
- Authentication only - no user lifecycle management
- Default IdP for HCP trial accounts

SAP Cloud Identity

- Cloud solution for Identity lifecycle management
- Pay-per-logon-requests (counted once per day and user)
- Isolated user base per tenant
- User import and export
- Rich customization and branding features
- Main scenarios: B2C and B2B
- Pre-configured trusted IdP for productive HCP accounts



“Bring your own identity provider”

- Prerequisite: SAML 2.0 compliance
- Main scenario: B2E
- * Product-specific support for authentication mechanisms, such as Kerberos, X.509, …

Summary

Administrators

- No need to manage a separate user store for cloud-based applications
- No user provisioning required
- Wide range of options for implementing the IdP
- Integration with IdP via well-known and proven security protocols

Developers

- Out-of-the-box integration for authentication and SSO
- No coding required – configuration only
- Simple APIs for Java, HTML5 and HANA XS to retrieve federated user attributes

Users

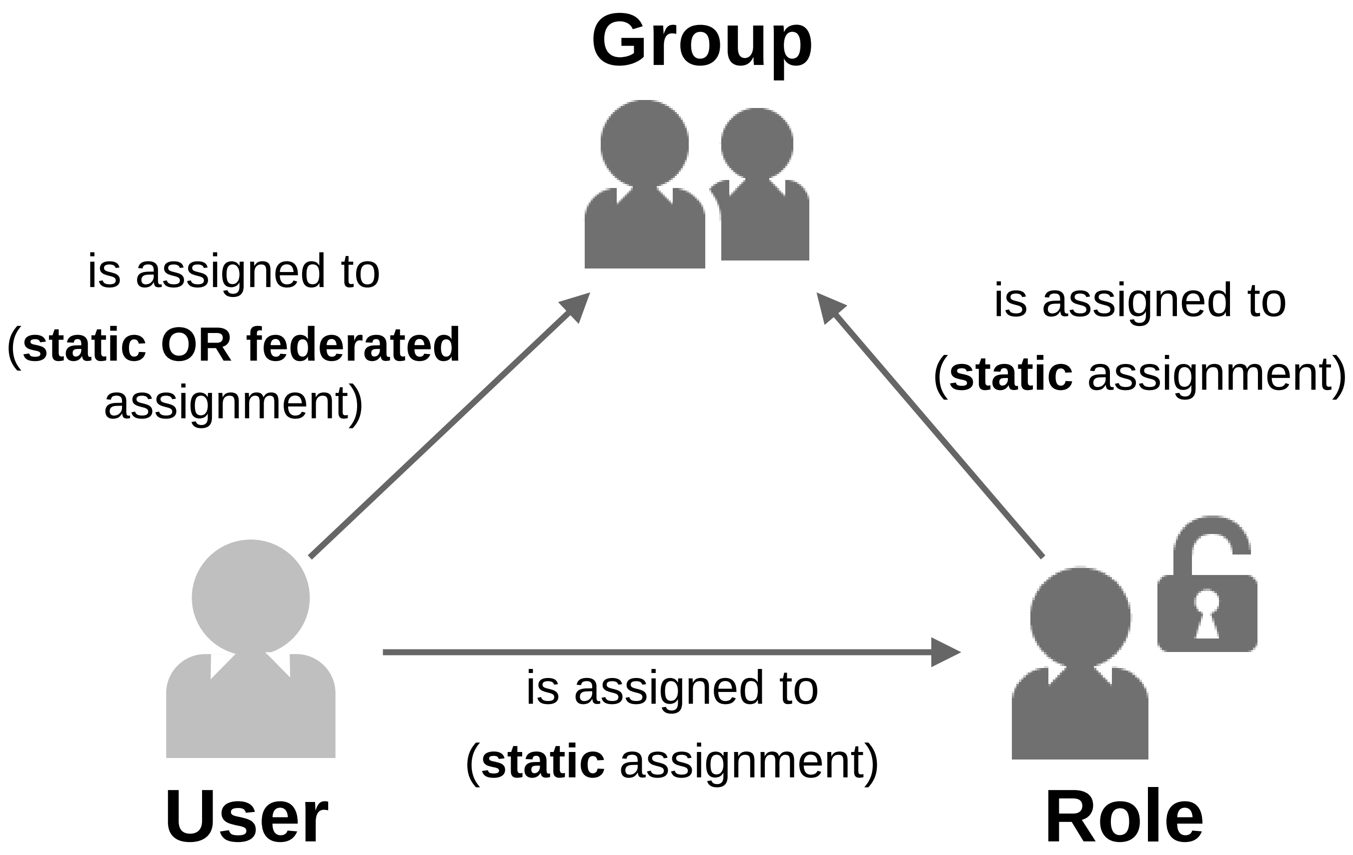
- Single sign-on to browser-based applications running on HCP
- No need for a separate user account and password in the cloud

Demo

Identity Provider Integration

Authorization management

User, role & group



Group

is assigned to

(**static OR federated** assignment)

is assigned to

(**static** assignment)

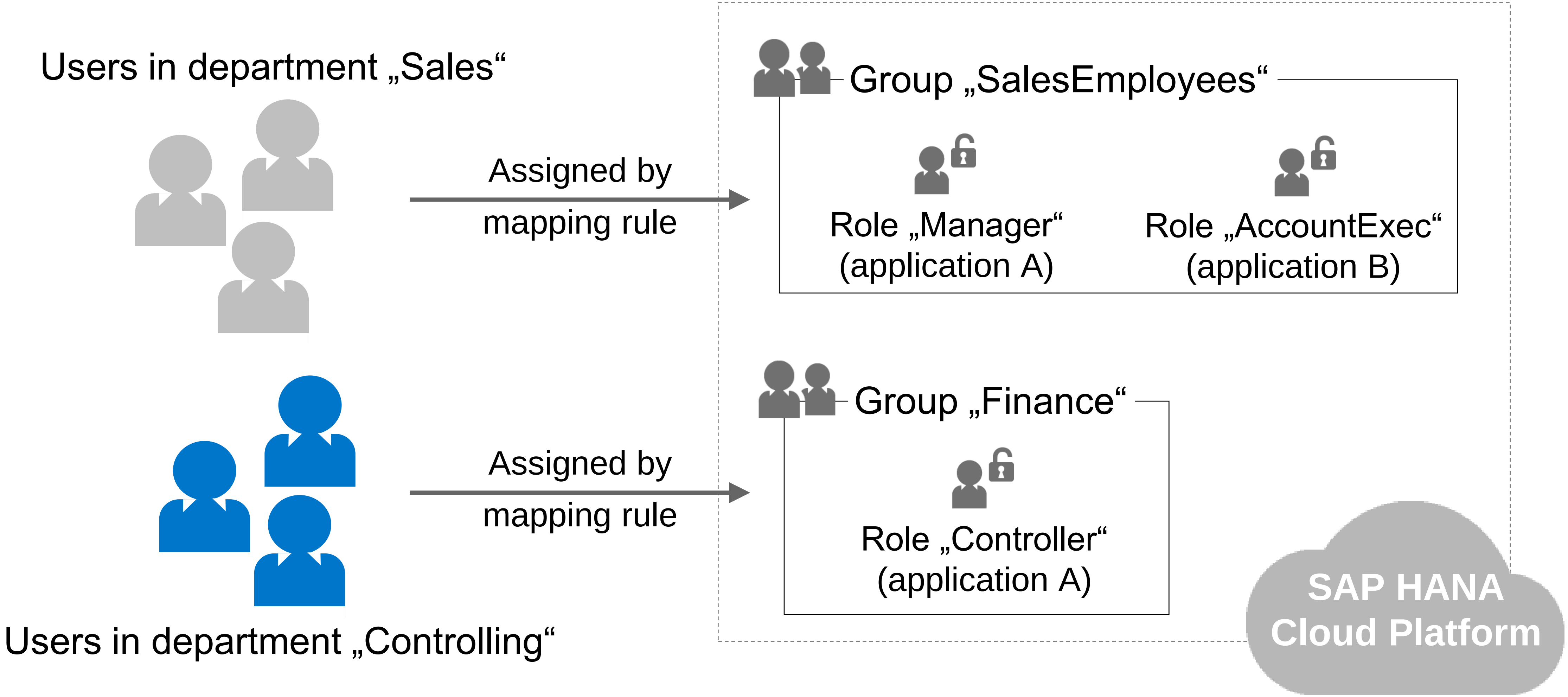
is assigned to

(**static** assignment)

User

Role

Federated authorization



Users in department „Sales“

Assigned by mapping rule

Group „SalesEmployees“

Role „Manager“ (application A)

Role „AccountExec“ (application B)

Users in department „Controlling“

Assigned by mapping rule

Group „Finance“

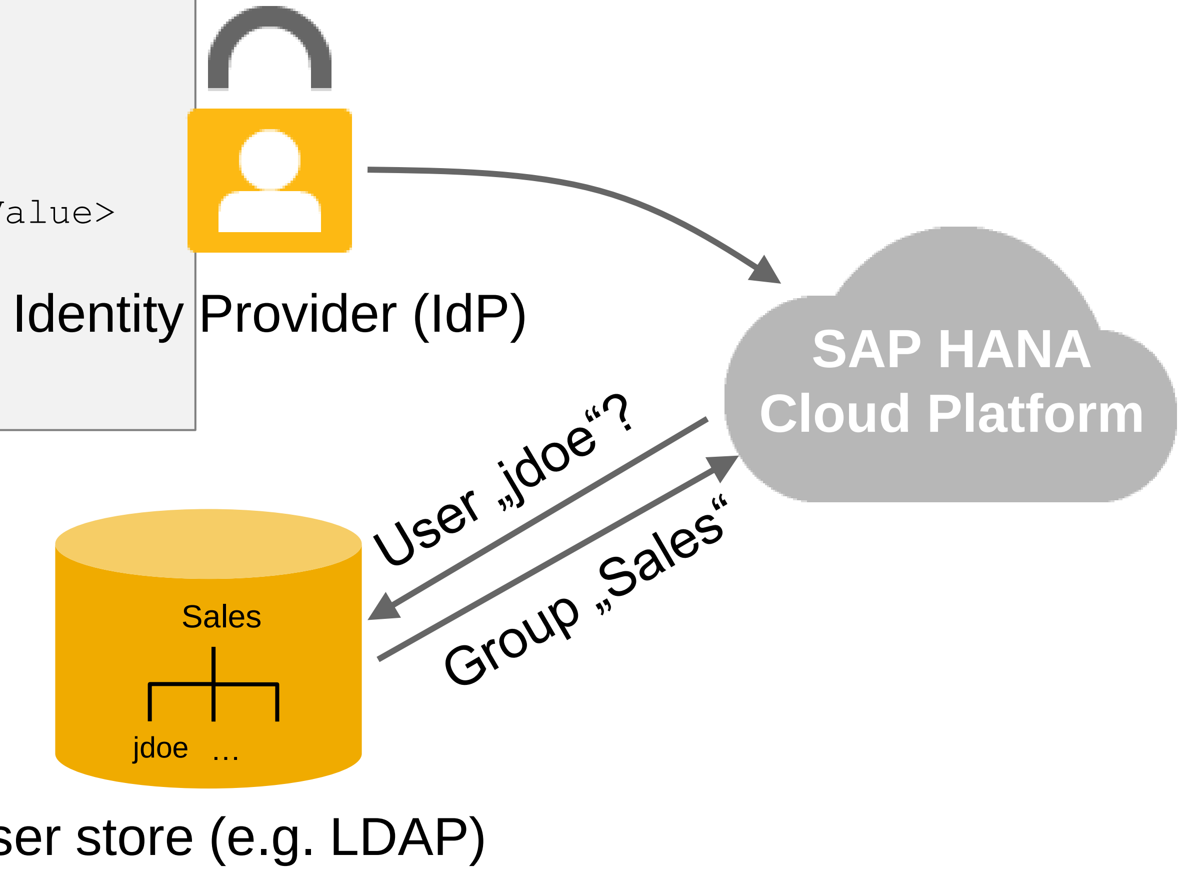
Role „Controller“ (application A)

SAP HANA Cloud Platform

Sources for federated role authorizations

SAML

```
<Response ...>
  ...
  <NameID>jdoe</NameID>
  ...
  <Attribute Name="department">
    <AttributeValue>Sales</AttributeValue>
  </Attribute>
  ...
</Response>
```



Authorization models in SAP HANA Cloud Platform

Runtime	Java	SAP XS	HTML 5
Authorization objects	• Java EE Roles (`web.xml`) • Custom roles (Cloud cockpit)	• Privileges (`.xsprivileges`) • Roles (`.hdbrole`)	• Permissions (`neo-app.json`) • Custom roles (Cloud cockpit)
Authorization management	• Static • Dynamic (federated authorizations)	• Static	• Static • Dynamic (federated authorizations)

Simplify integration of HCP with your applications using the security platform APIs

- **Authorization management API**

  Management of users, roles, groups and their assignments within the account

- **Trust management API***

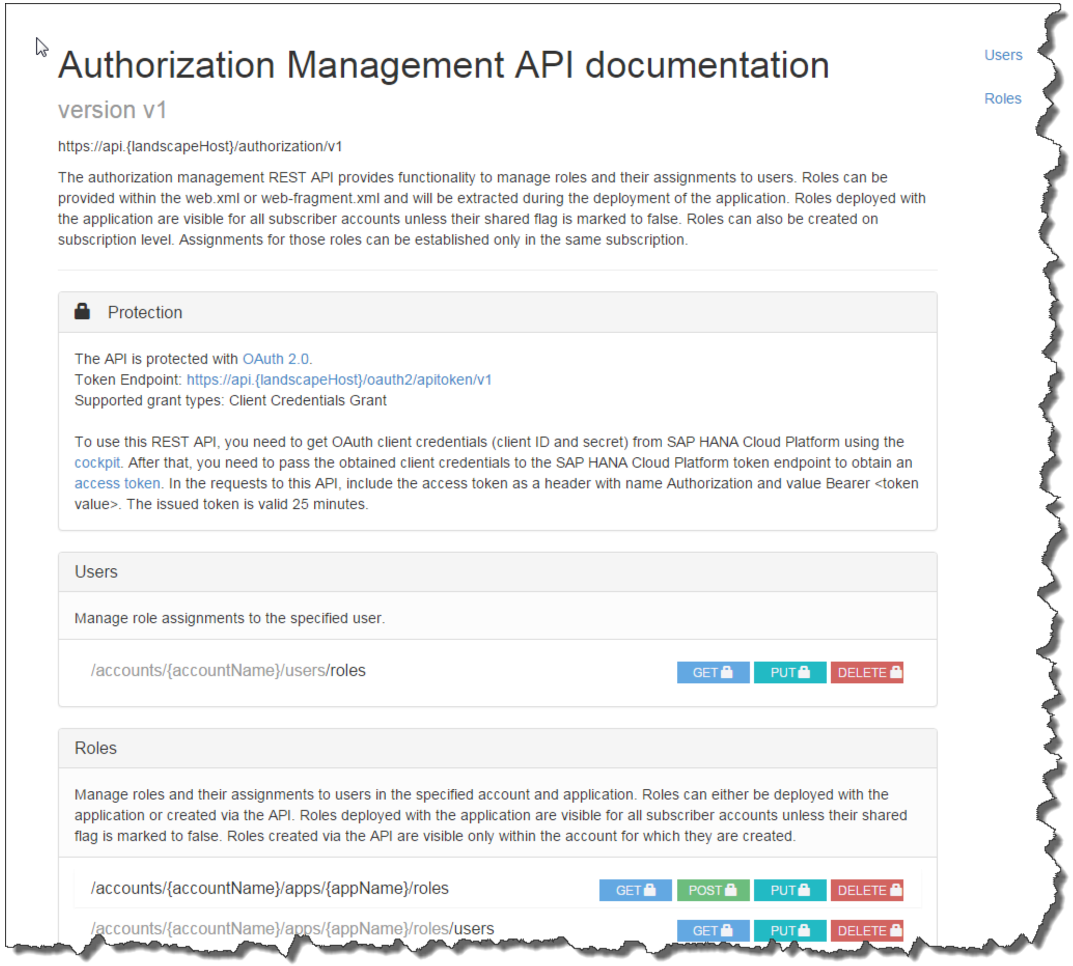
  Management of SAML2 trust settings such as local service provider and trusted providers within the account

- **OAuth client management API ***

  Management of OAuth clients, scopes and access tokens for an account

APIs are protected with OAuth 2.0

https://api.hana.ondemand.com/authorization/v1/documentation



Authorization Management API documentation

version v1

https://api.{landscapeHost}/authorization/v1

The authorization management REST API provides functionality to manage roles and their assignments to users. Roles can be provided within the web.xml or web-fragment.xml and will be extracted during the deployment of the application. Roles deployed with the application are visible for all subscriber accounts unless their shared flag is marked to false. Roles can also be created on subscription level. Assignments for those roles can be established only in the same subscription.

Protection

The API is protected with OAuth 2.0.
Token Endpoint: https://api.{landscapeHost}/oauth2/apitoken/v1
Supported grant types: Client Credentials Grant

To use this REST API, you need to get OAuth client credentials (client ID and secret) from SAP HANA Cloud Platform using the cockpit. After that, you need to pass the obtained client credentials to the SAP HANA Cloud Platform token endpoint to obtain an access token. In the requests to this API, include the access token as a header with name Authorization and value Bearer <token value>. The issued token is valid 25 minutes.

Users

Manage role assignments to the specified user.

/accounts/{accountName}/users/roles

Roles

Manage roles and their assignments to users in the specified account and application. Roles can either be deployed with the application or created via the API. Roles deployed with the application are visible for all subscriber accounts unless their shared flag is marked to false. Roles created via the API are visible only within the account for which they are created.

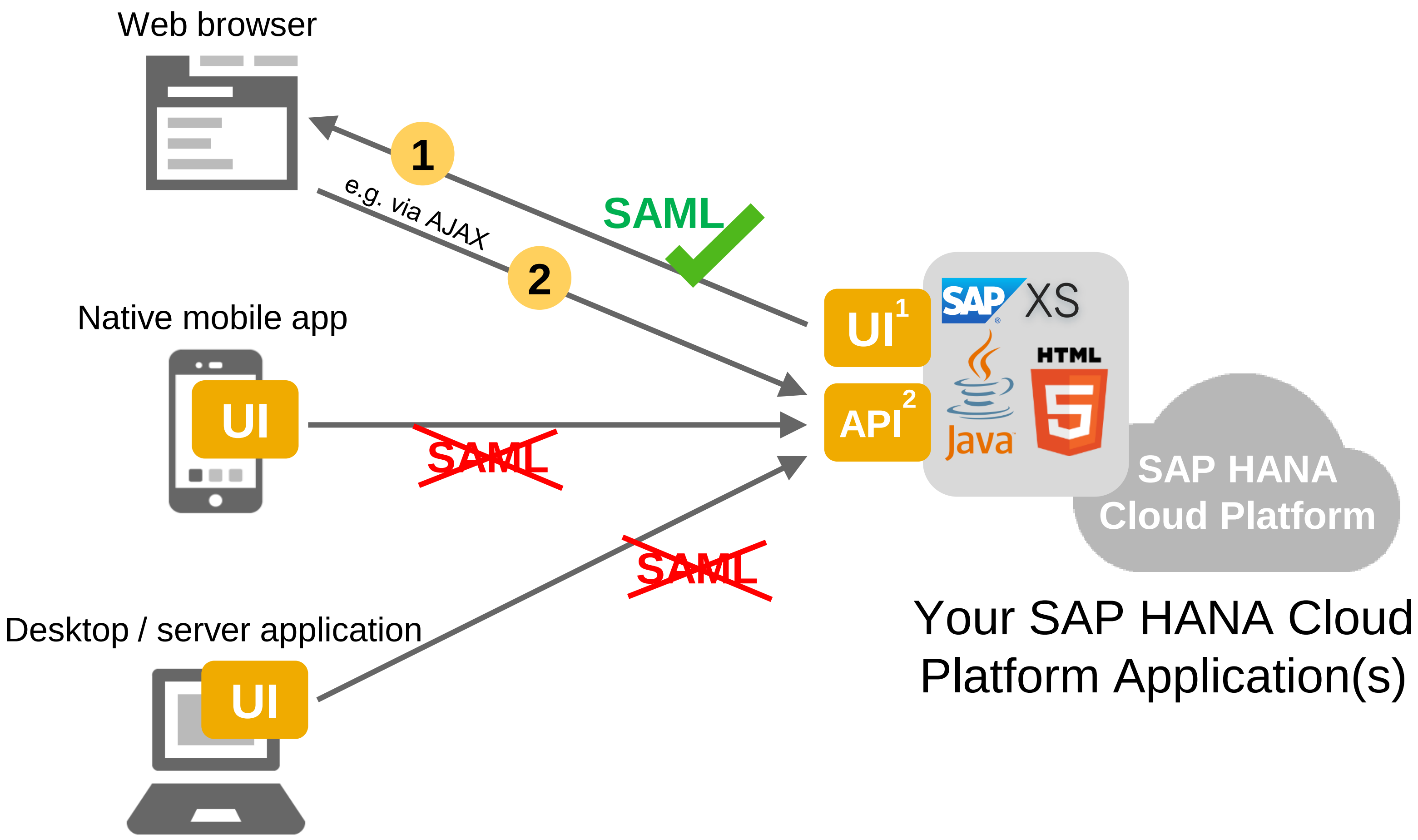
/accounts/{accountName}/apps/{appName}/roles

/accounts/{accountName}/apps/{appName}/roles/users

* planned innovations / future direction

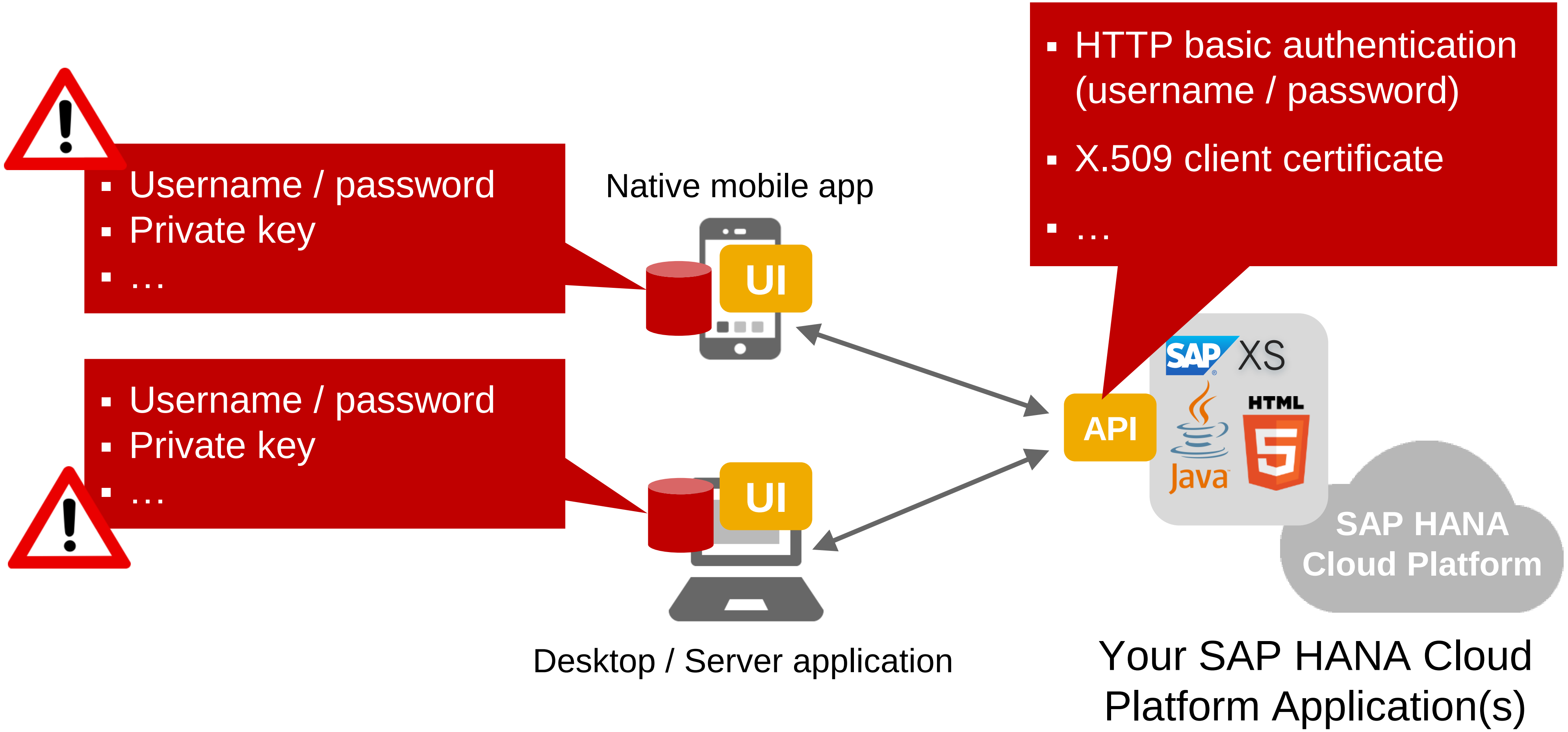
API protection

API scenario



1) User Interface 2) (RESTful) Application Programming Interface

How to protect an API for non-browser based clients?



- HTTP basic authentication (username / password)
- X.509 client certificate
- …

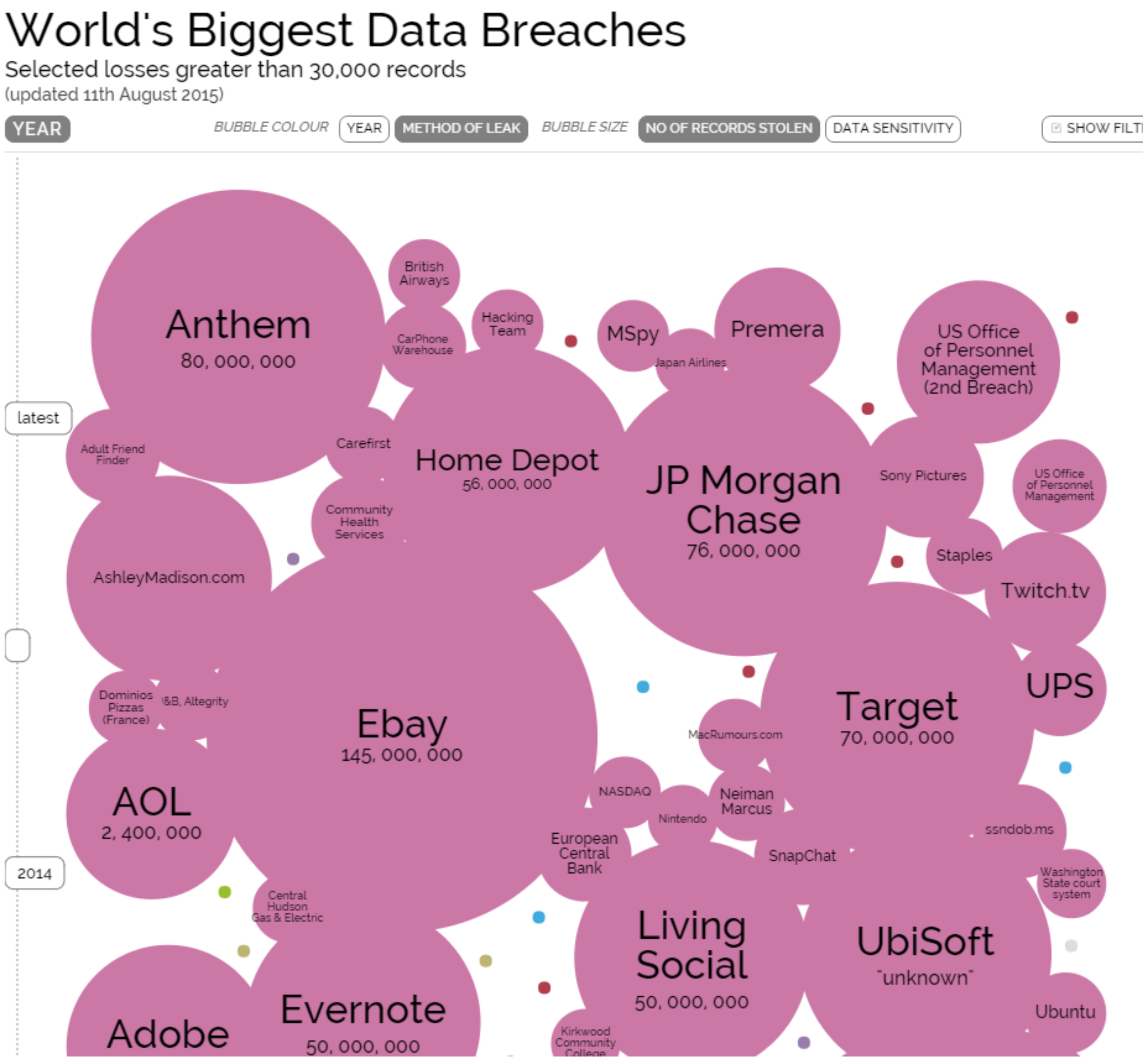
- Username / password
- Private key
- …

- Username / password
- Private key
- …

Your SAP HANA Cloud Platform Application(s)

The issues caused by stolen user credentials are huge…

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



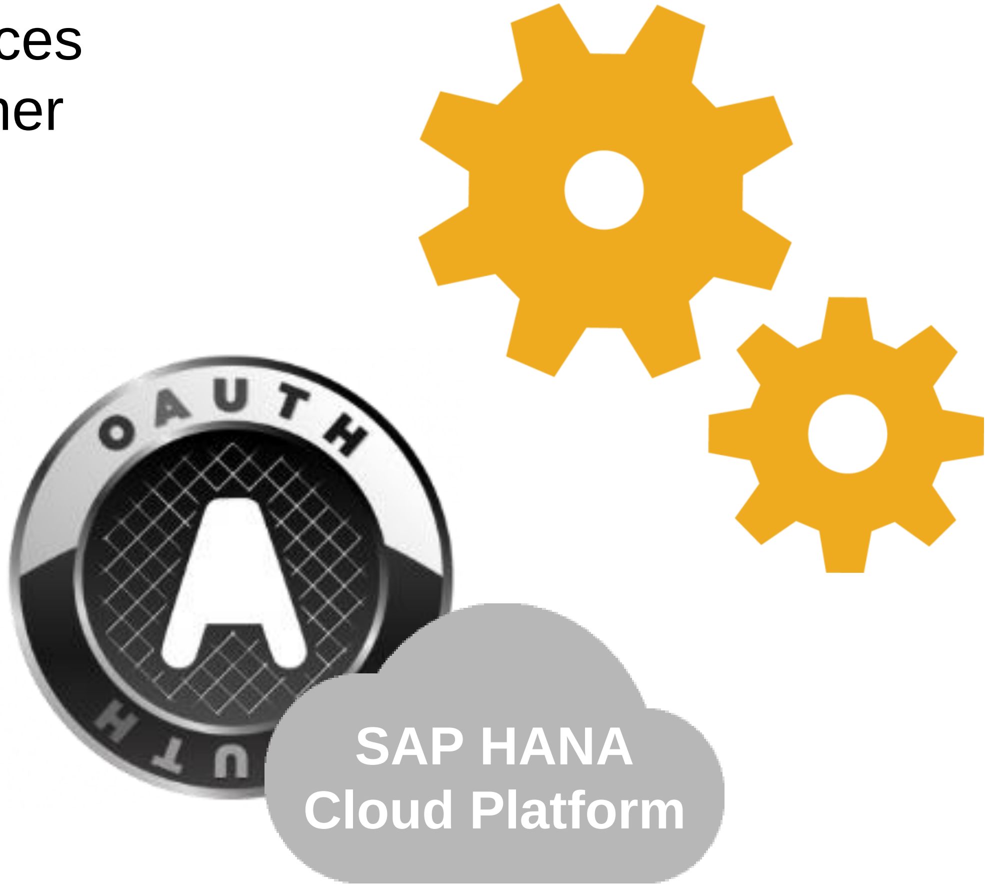
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 11th August 2015)

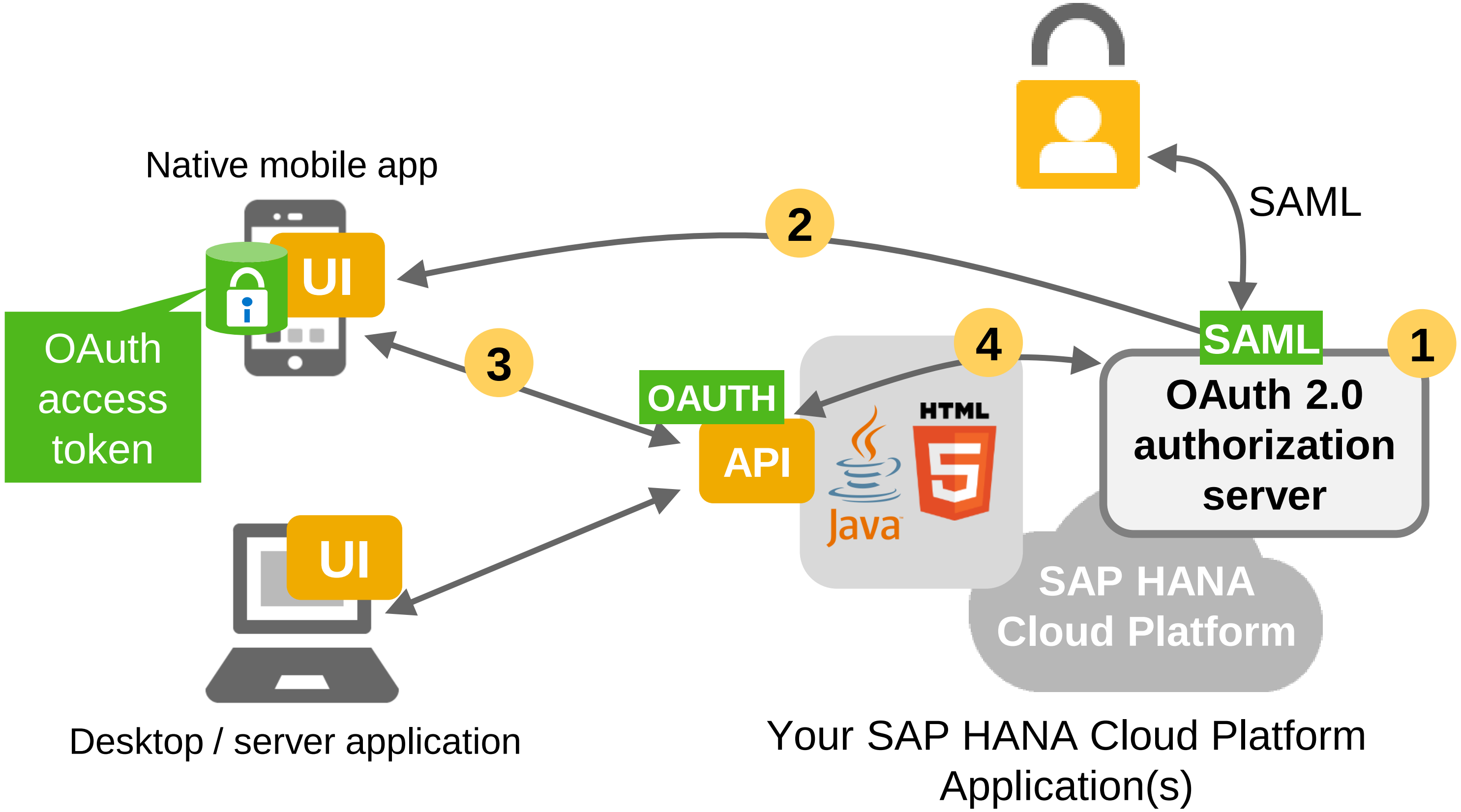
OAuth to the rescue!

- OAuth can **grant a client access** to protected resources **without sharing the credentials** of the resource owner
- OAuth 2.0 is specified in IETF **RFC 6749**
- OAuth replaces the user‘s username and password with a **token**
- Although the token is **still vulnerable to theft**, it has a very **narrow scope** compared to the user‘s password
- It only allows a specific client to access a specific resource
- The **user is in full control** at any time **to revoke** the granted access to the client



The HCP OAuth 2.0 authorization server

1. Administrator registers OAuth client for the app(s)
2. App requests an access token from the OAuth authorization server. This requires the user to authenticate via SAML.
3. App stores the access token and uses it to send an authorized API call
4. The API can verify* the token with the OAuth authorization server and returns the response to the app


Native mobile app
UI
OAuth access token
2
3
4
1
SAML
SAML
OAUTH
API
HTML 5
Java
OAuth 2.0 authorization server
SAP HANA Cloud Platform
UI
Desktop / server application
Your SAP HANA Cloud Platform Application(s)

* only supported for Java and HTML5-based applications, and not supported for HANA XS

Storing confidential data

Storing confidential data on SAP HANA Cloud Platform

Password storage

- Securely persist strings such as passwords for keystore files or OAuth access tokens
- Persisted strings survive application restarts and updates and stay persisted unless you explicitly delete them via the API, or you undeploy your application
- Password storage is exposed to applications* via a programmatic API

SAP HANA Cloud Platform

Keystore service

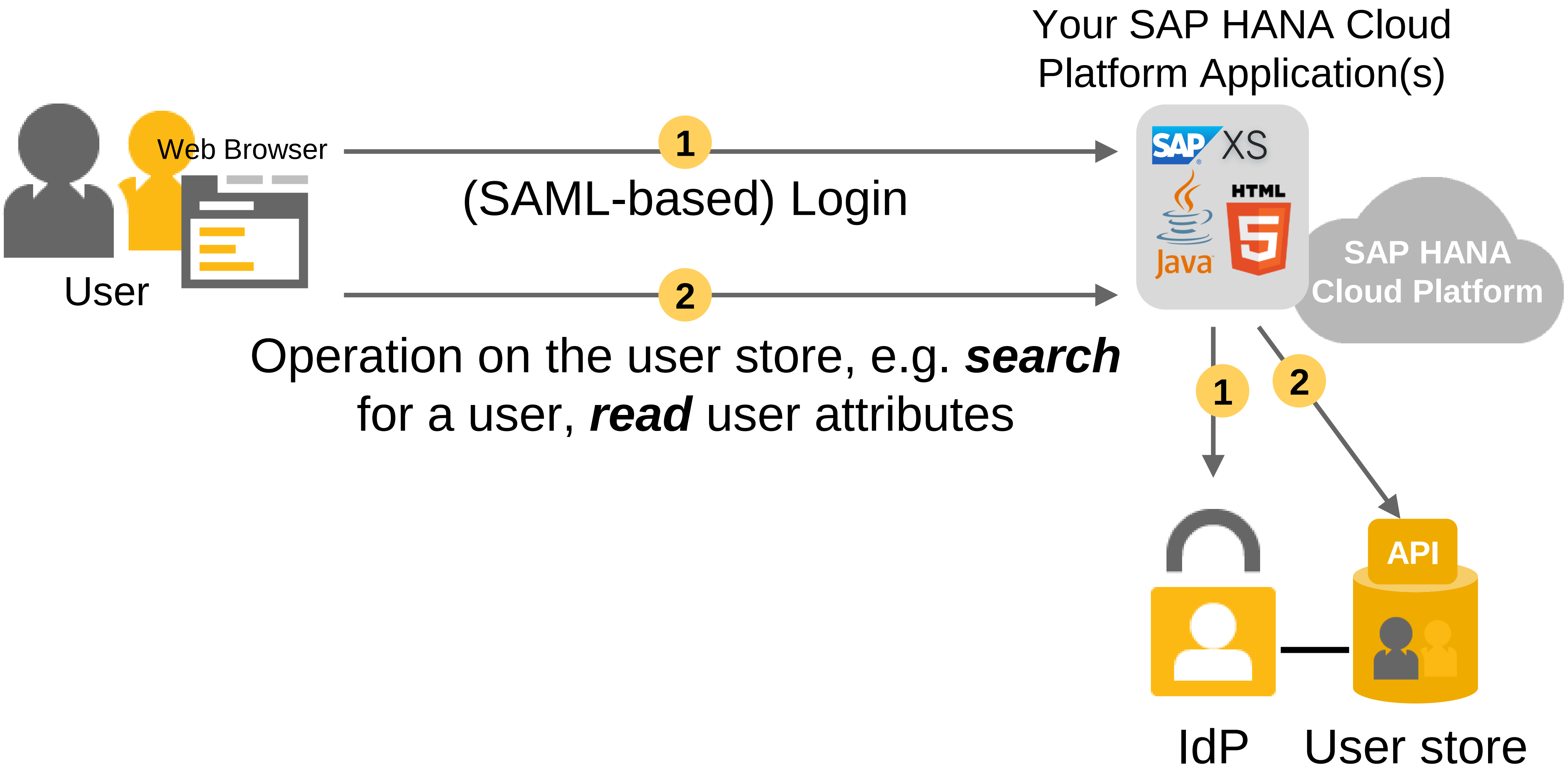
- Provides a repository for cryptographic keys and certificates to the applications hosted on SAP HANA Cloud Platform
- Keystores can be used for various cryptographic operations such as signing and verifying of digital signatures, encrypting and decrypting messages, and performing SSL communication
- Keystore service is exposed to applications* via a programmatic API

* Password storage and keystore service are supported on Java and HTML5 runtime only. For managing keys and certificates in HANA XS applications, refer to HANA Trust Stores

User store integration

Public

User store integration scenario



Your SAP HANA Cloud Platform Application(s)

(SAML-based) Login

Operation on the user store, e.g. ***search*** for a user, ***read*** user attributes

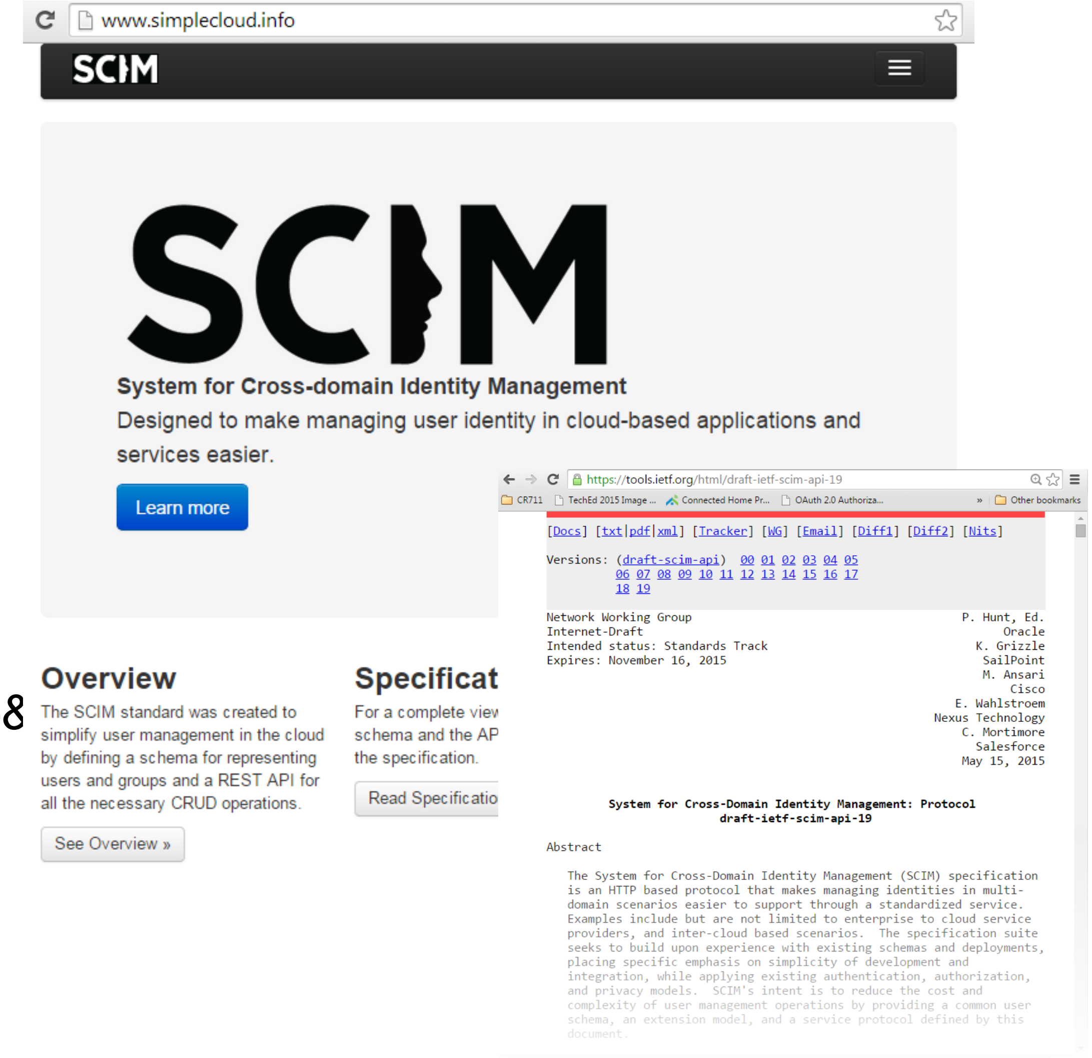
SCIM to the rescue!

SCIM provides a **REST API** with a rich but simple set of operations for managing user identities

- Create = POST https://example.com/{v}/{resource}
- **Read**[1] = GET https://example.com/{v}/{resource}/{id}
- Replace = PUT https://example.com/{v}/{resource}/{id}
- Delete = DELETE https://example.com/{v}/{resource}/{id}
- Update = PATCH https://example.com/{v}/{resource}/{id}
- **Search**[1] = GET

  https://example.com/{v}/{resource}?filter={attribute}{op}{value}&

  rtBy={attributeName}&sortOrder={ascending|descending}
- Bulk = POST https://example.com/{v}/Bulk



System for Cross-domain Identity Management

Designed to make managing user identity in cloud-based applications and services easier.

Overview

The SCIM standard was created to simplify user management in the cloud by defining a schema for representing users and groups and a REST API for all the necessary CRUD operations.

Specificat

For a complete view schema and the AP the specification.

```
[Docs] [txt|pdf|xml] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-scim-api)  00 01 02 03 04 05
          06 07 08 09 10 11 12 13 14 15 16 17
          18 19

Network Working Group                                       P. Hunt, Ed.
Internet-Draft                                                    Oracle
Intended status: Standards Track                              K. Grizzle
Expires: November 16, 2015                                     SailPoint
                                                               M. Ansari
                                                                   Cisco
                                                            E. Wahlstroem
                                                       Nexus Technology
                                                            C. Mortimore
                                                              Salesforce
                                                            May 15, 2015


          System for Cross-Domain Identity Management: Protocol
                        draft-ietf-scim-api-19

Abstract

   The System for Cross-Domain Identity Management (SCIM) specification
   is an HTTP based protocol that makes managing identities in multi-
   domain scenarios easier to support through a standardized service.
   Examples include but are not limited to enterprise to cloud service
   providers, and inter-cloud based scenarios.  The specification suite
   seeks to build upon experience with existing schemas and deployments,
   placing specific emphasis on simplicity of development and
   integration, while applying existing authentication, authorization,
   and privacy models.  SCIM's intent is to reduce the cost and
   complexity of user management operations by providing a common user
   schema, an extension model, and a service protocol defined by this
   document.
```

[1] Currently supported operations in HCP

Supported user stores via SCIM on SAP HANA Cloud Platform

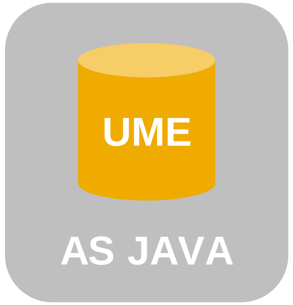
Cloud

SAP Cloud Identity

On-Premise

Corporate LDAP
(Microsoft Active Directory)

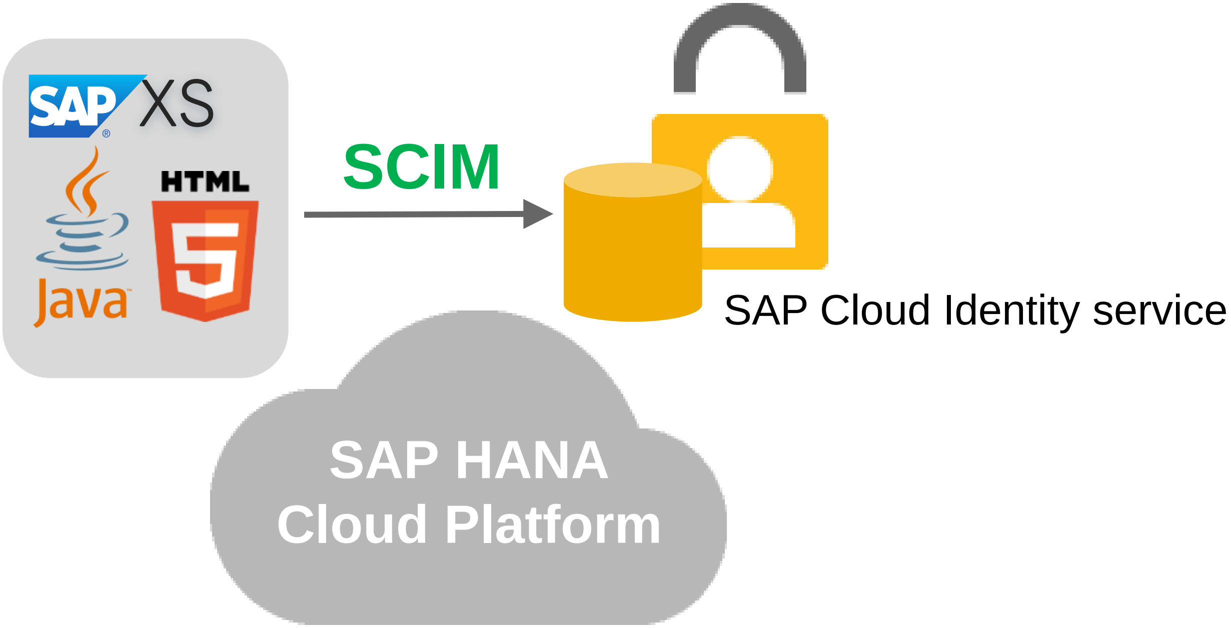
SAP NetWeaver
AS ABAP



SAP NetWeaver
AS JAVA

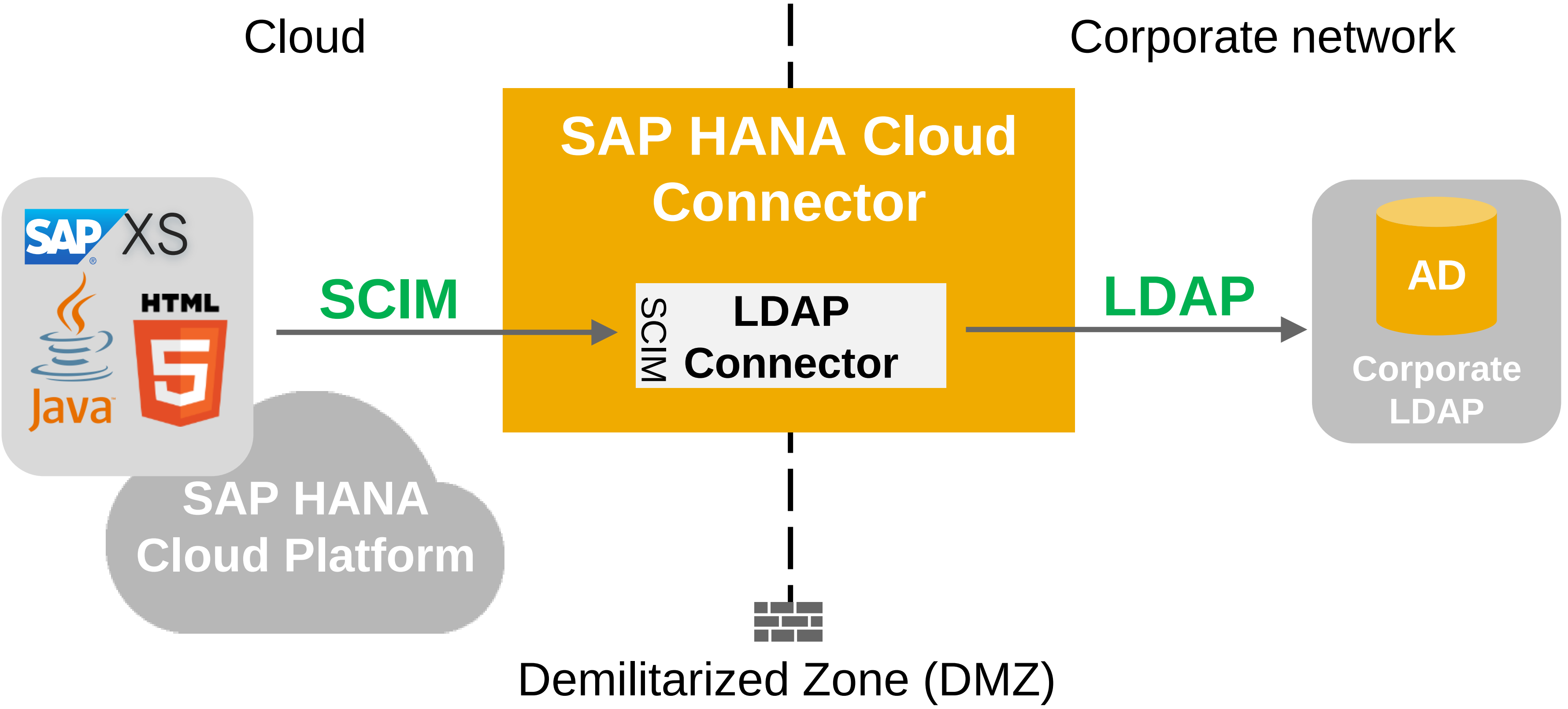
Setup of a SCIM-based user store integration

with SAP Cloud Identity service



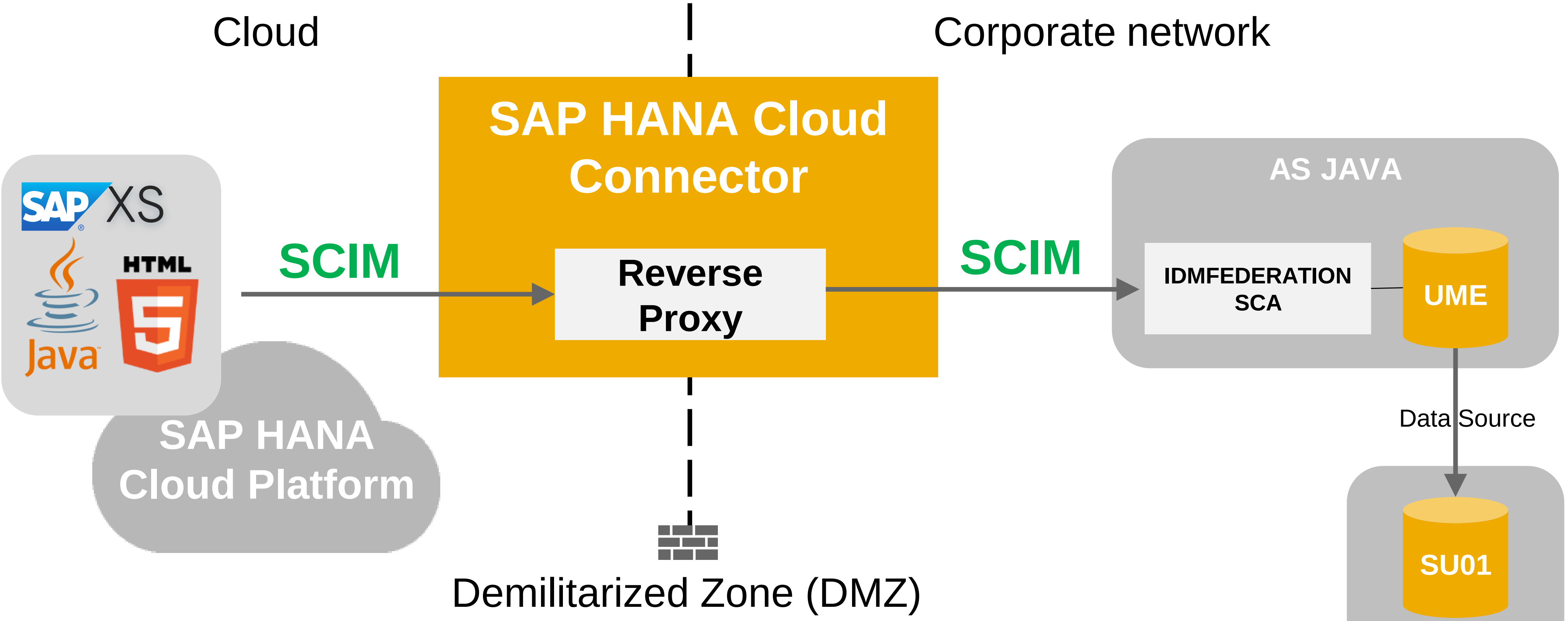
Setup of a SCIM-based user store integration

with Microsoft Active Directory



Setup of a SCIM-based user store integration

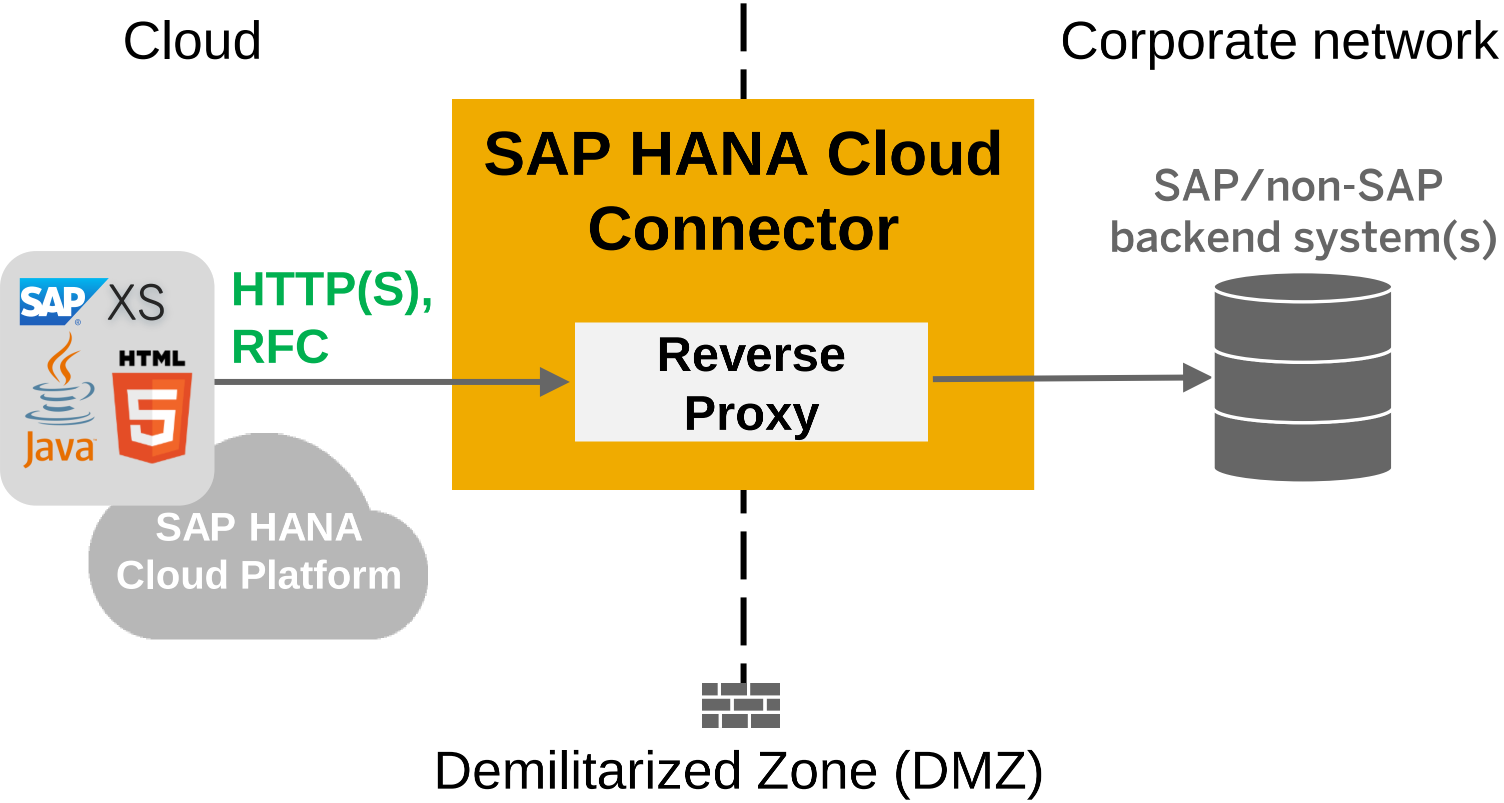
with SAP NetWeaver AS ABAP



Secure backend connectivity

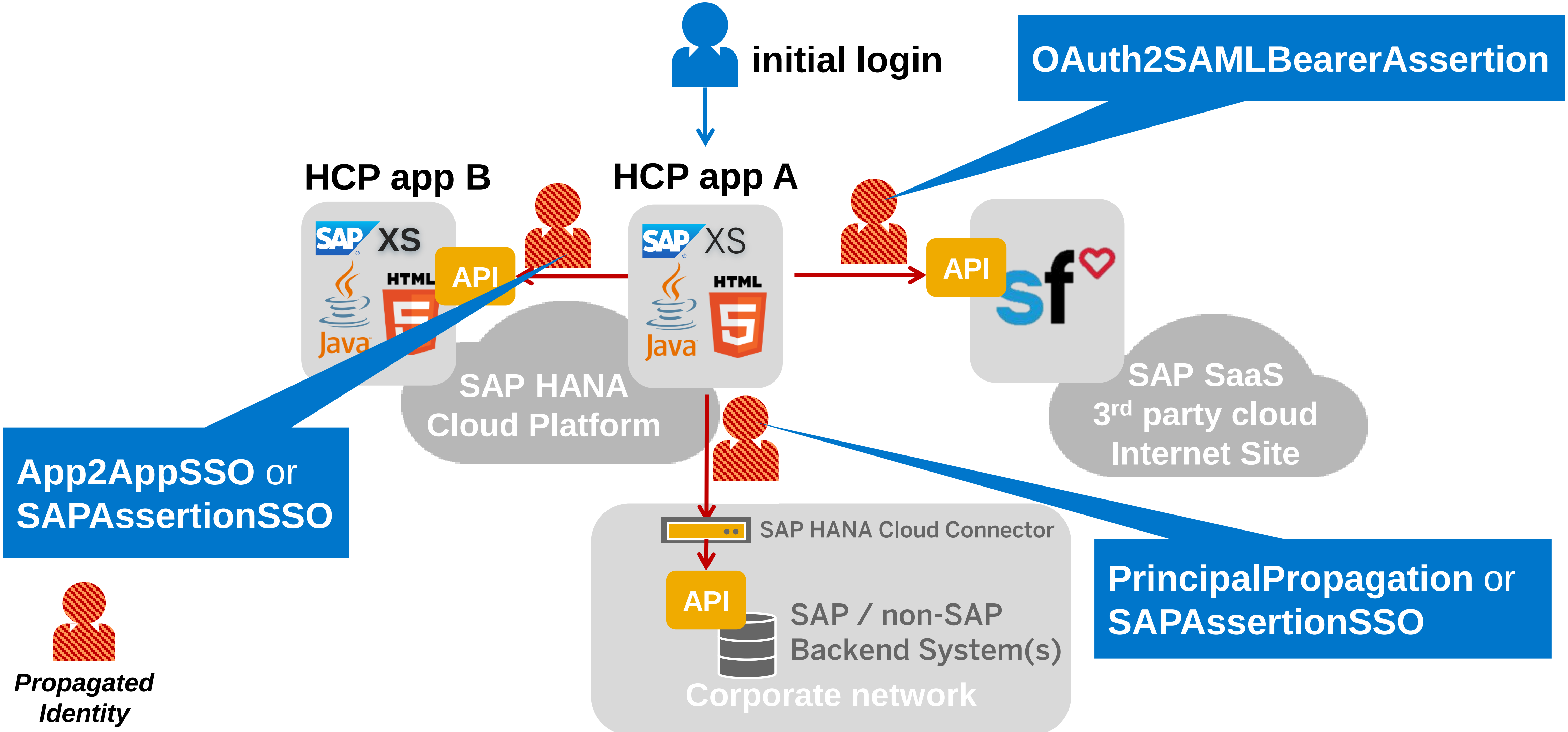
Secure backend connectivity with the SAP HANA Cloud Connector

- Establishes **secure VPN connection** between the SAP HANA Cloud Platform and on-premise systems
- Connectivity created by on-premise agent **through reverse-invoke process**
- Supports pre-configured “destination API” and certificate inspection to safeguard against forgeries
- Complementary to SAP Gateway, HANA Cloud Integration and 3rd party integration suites both on-premise and in the cloud



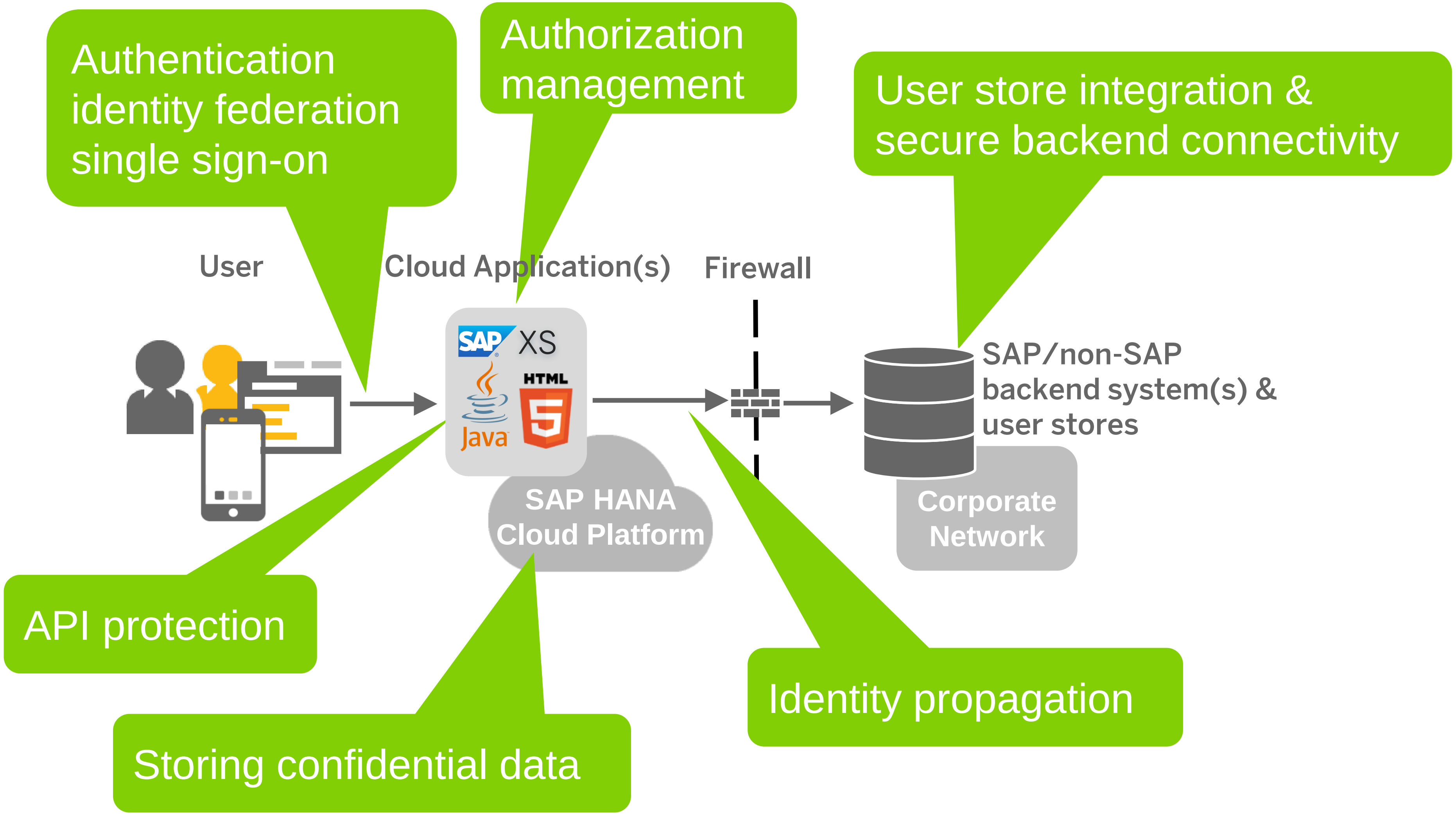
Identity propagation

Supported identity propagation scenarios on HCP



Summary

Summary



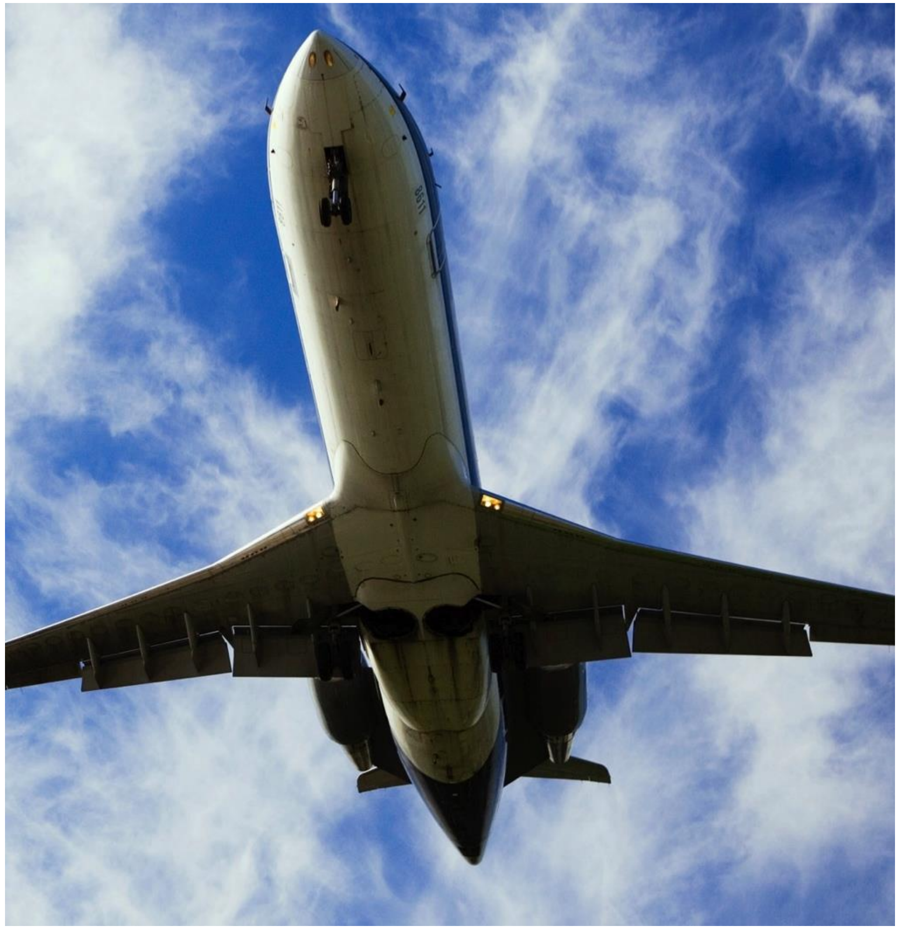
Authentication
identity federation
single sign-on
Authorization
management
User store integration &
secure backend connectivity
User
Cloud Application(s)
Firewall
XS
HTML
Java
SAP HANA
Cloud Platform
SAP/non-SAP
backend system(s) &
user stores
Corporate
Network
API protection
Storing confidential data
Identity propagation

What you have learned in this session

SAP HANA Cloud Platform is SAP‘s PaaS solution, providing a rich set of security services to build, extend and integrate secure cloud applications

All security services are based on open standards, such as SAML 2.0, OAuth 2.0 and SCIM 1.1

→ Get started today!



Further Information

Related SAP TechEd 2015 sessions:

DEV263 - Cloud Security: Using the Security Services in SAP HANA Cloud Platform

SEC704 - Defend Your SAP HANA Cloud Platform Application Against Cyber Attacks

EXP27160 & EXP27163 – Cloud Security Q&A (Networking Sessions)

DEV266 - Extend the Reach of your SAP Installed Base with SAP HANA Cloud Platform

DEV101 - Extending SAP Business Suite and SAP S/4HANA with SAP HANA Cloud Platform

DEV102 - SAP HANA Cloud Platform: A Guided Tour

DEV300 - Architecture Guidelines for Microservices Based on SAP HANA Cloud Platform

DEV165 - Extending SAP Cloud Solutions Using SAP HANA Cloud Platform

SAP Public Web

SAP HANA Cloud Platform Developer Center

SAP HANA Cloud Platform Security Tutorial Series

openSAP Courses

https://open.sap.com/courses/hanacloud1 and https://open.sap.com/courses/hanacloud2

Thank you

Contact information:

Martin Raepple
martin.raepple@sap.com

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see http://global12.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.